ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 28 МАТЕМАТИКИ Выпуск 2
2021

В. А. Едемский (Великий Новгород, НовГУ). **О m-адической сложности четвертичных последовательностей с периодом pq.**

УДК 519.7

Резюме: Исследована m-адическая сложность четвертичных последовательностей, период которых равен произведению двух простых чисел. Показано, что рассматриваемые последовательности имеют высокую симметричную m-адическую сложность.

Ключевые слова: m-адическая сложность, четвертичные последовательности.

Работа посвящена анализу m-адической сложности четвертичных последовательностей, период которых равен произведению двух простых чисел. Четвертичные последовательности, наряду с бинарными и троичными, относятся к наиболее востребованным в приложениях. m- адическая сложность последовательности определяется как наименьшая длина регистра сдвига с обратной связью по переносу (feedback with carry shift register), порождающего последовательность, и является важной характеристикой последовательности [**?**]. Если $s^\infty = (s_0, s_1, \ldots, s_{N-1})$ — последовательность с периодом N над кольцом классов вычетов $\mathbb{Z}_m$ по модулю $m, m > 1$ и $S(x) = \sum_{i=0}^{N-1} s_i x^i \in \mathbb{Z}[x]$ — порождающий многочлен последовательности, то её m-адическая сложность может быть определена по следующей формуле:

$$\Phi_m(s^\infty) = \left\lfloor \log_m \left(\frac{m^N - 1}{\gcd\left(S(m), m^N - 1\right)} + 1 \right) \right\rfloor,$$

где $\lfloor x \rfloor$ — наибольшее целое число, меньшее или равное x [**?**].

Бинарные и другие последовательности также могут рассматриваться как последовательности над $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$. В этом случае, для каждого m имеем новую характеристику последовательности. Согласно [**?**], последовательности с низкой m-адической сложностью не подходят для криптографических приложений. Таким образом, представляет интерес поиск последовательностей с высокой m-адической сложностью. Исследование m-адической сложности ряда бинарных последовательностей выполнено в [**?**].

Пусть p и q — простые числа, такие что НОД$(p-1, q-1) = 4$ и $e = (p-1)(q-1)/4$. Обозначим через g общий примитивный корень по модулям p и q. Обобщенные циклотомические классы четвертого порядка по модулю pq определяются как:

$$D_i = \{g^j h^i : j = 0, 1, \ldots, e-1\}, \qquad i = 0, 1, 2, 3,$$

где h : $h \equiv g \pmod p$ и $h \equiv 1 \pmod q$. Дополнительно введем следующие обозначения: $P = \{p, 2p, \ldots, (q-1)p\}$, $Q = \{0, q, 2q, \ldots, (p-1)q\}$. Тогда справедливы разбиения:

$$\mathbb{Z}_{pq}^* = \bigcup_{i=0}^{3} D_i \quad \text{и} \quad \mathbb{Z}_{pq} = \bigcup_{i=0}^{3} D_i \cup P \cup Q.$$

© Редакция журнала «ОПиПМ», 2021 г.

Четвертичная последовательность $s^\infty = (s_0, s_1, s_2, \dots)$ с периодом pq может быть определена по следующей формуле:

$$s_i = \begin{cases} 0, & \text{если } i \pmod{pq} \in P, \\ 2, & \text{если } i \pmod{pq} \in Q, \\ j, & \text{если } i \pmod{pq} \in C_j. \end{cases} \quad (1)$$

Линейная сложность этой последовательности и её автокорреляция изучены ранее. Четвертичную последовательность s^∞ также можно рассматривать как последовательность над кольцом $\mathbb{Z}_m$ для $m \geqslant 4$. В этой работе исследована m-адическая сложность таких последовательностей. Метод анализа основан на свойствах полиномов Холла рассматриваемых последовательностей. Показано, что последовательности имеет высокую m-адическую сложность для любых значений простых чисел p, q. В частности, справедливо следующее утверждение.

Теорема *Пусть* s^∞ *— четвертичная последовательность с периодом* $£pq$, (**??**) $m \geqslant 4$. *Тогда для её* m*-адической сложности имеет место следующая оценка:* $\Phi_m(s^\infty) \geqslant pq - \log_4 \max(p^2q^3, p^3q^2) - 2$.

Также изучена симметричная m-адическая сложность рассматриваемых последовательностей. Обобщены результаты о 4-адической сложности четвертичных последовательностей, полученные в [**?**].

СПИСОК ЛИТЕРАТУРЫ

1. *Edemskiy V.*, *Chen Z.* On the 4-adic complexity of the two-prime quaternary generator. — arXiv:2106.05483 [cs.CR] 10 Jun 2021.
2. *Jing X.*, *Xu Z.*, *Yang M.*, *Feng K.* On the p-Adic Complexity of the Ding-Helleseth-Martinsen Binary Sequences. — Chinese Journal of Electronics, 2021, v. 30, № 1, p. 64–71.
3. *Xu J.*, *Klapper A.* Feedback with carry shift registers over $\mathbb{Z}/(N)$. — SETA 1998, p. 379–392.

UDC 519.7

Edemskiy V. A. (Veliky Novgorod, Yaroslav-the-Wise Novgorod State University).
About the m-adic complexity of quaternary sequences with period pq.

Abstract: The m-adic complexity of quaternary sequences with a period equal to the product of two primes is studied. It is shown that these sequences have high symmetric m-adic complexity.

Keywords: m-adic complexity, quaternary sequences.